



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/066,070 | 02/01/2002 | Satyendra Yadav | 10559-754001 | 2485 |

20985 7590 03/05/2009
FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

| |
|----------|
| EXAMINER |
|----------|

TRUVAN, LEYNNA THANH

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2435

| | |
|-------------------|---------------|
| NOTIFICATION DATE | DELIVERY MODE |
|-------------------|---------------|

03/05/2009

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

| | | | |
|--|--------------------------------------|---|--|
| <p align="center">Advisory Action Before the Filing of an Appeal Brief</p> | Application No. 10/066,070 | Applicant(s) YADAV, SATYENDRA | |
| | Examiner Leynna T. Truvan | Art Unit 2435 | |

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 09 February 2009 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☐ The period for reply expires _____ months from the mailing date of the final rejection.
 b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
 (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
 (b) ☐ They raise the issue of new matter (see NOTE below);
 (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
 (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
 5. ☐ Applicant's reply has overcome the following rejection(s): _____.
 6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
 7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
 The status of the claim(s) is (or will be) as follows:
 Claim(s) allowed: _____.
 Claim(s) objected to: _____.
 Claim(s) rejected: 21-28.
 Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
 9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
 10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Continuation Sheet.
 12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____.
 13. ☐ Other: _____.

/Kimyen Vu/
 Supervisory Patent Examiner, Art Unit 2435

Continuation of 11. does NOT place the application in condition for allowance because: claims remains rejected in view of Kouznetsov and Gryaznov.

Regarding the argument on pg.2, that Kouznetsov does not teach obtaining application-specific intrusion criteria and points to abstract. The details of the abstract alone does not fully provide the entirety of Kouznetsov's invention, thus, there includes background and specification further explaining with more details of his invention.

Regarding the argument on pg.3, that the specific event sequence characteristics of computer virus behavior does not constitute intrusion criteria but rather is the output of the tracking performed using intrusion criteria. Examiner broadly and reasonable interprets intrusion criteria as something that is harming or causing unsafe, malware, intruders, or viruses. As such application specific intrusion criteria can be given as virus behavior and the application that performed the specific event sequence reads on the claimed as application intrusion criteria.

Regarding the argument on pg.4, that the present claims do not state that intrusion criteria are tracked and contrary specifies that network communications for the invoked application are monitored using the application specific intrusion criteria. However, claim 21 includes examining an invoked application to identify it, obtaining application specific intrusion criteria, and specifically recites "monitoring network communications for the invoked application". Thus, it is not as applicant stated as "using" the application specific intrusion criteria but monitoring "for" the invoked application as claimed. Additionally, monitoring can broadly be interpreted as a form of tracking, filtering, load balancing, and other techniques requiring to go through and examine incoming/outgoing communications/traffic.

Regarding the last paragraph of pg.4 that nowhere in Kouznetsov suggests determination of whether application is performing a sequence of "suspicious" actions characteristics of computer viruses is based on criteria specific to an application. According to claim 21, nowhere recites performing a sequence of "suspicious" actions characteristics of computer viruses is based on criteria specific to an application

Regarding the argument on pg.5, that neither Kouznetsov nor Gryaznov teaches or suggests the claimed examining a set of instructions embodying an invoked application to identify the invoked application. Kouznetsov as noted above teaches and suggests the application specific intrusion criteria by determining whether the application is performing a sequence of suspicious actions characteristic of computer viruses (col.2, lines 32-40 and col.4, lines 15-36). A (intrusive) criteria broadly and obviously can be any data/content that is considered to identify or measure what is deemed as intrusive or as an intrusion. In essence, examiner finds Kouznetsov suggest identifying an invoked application. However, examiner goes further to give the claimed "to identify the invoked application" can also be a form of literal identification or labeling the intrusion (i.e. as ID, name, number, etc.) so as "to identify the invoked application" of the intrusion criteria specific to an application. Hence, Gryaznov is combined with Kouznetsov to teach the obviousness of identifying the invoked application. Gryaznov discloses a method and system for providing computer malware names from multiple anti-virus scanners (col.1, lines 6-9) where an anti-virus scanner detect and identify viruses and other malwares (col.4, lines 7-10 and col.6, lines 5-15). The information identifying the computer malware may comprise a name of the computer malware and at least one of a computer virus, a computer worm, or Trojan horse program (col.2, lines 7-15). Hence, Gryaznov reads on the claimed identifying the invoked application, obtaining application-specific intrusion criteria and monitoring network communications for the invoked application, after the examining and the obtaining, using the application-specific intrusion criteria to detect an intrusion (col.2, lines 1-55). It would have been obvious for a person of ordinary skills in the art to combine the teachings of Kouznetsov with Gryaznov for identifying the invoked application because different anti-virus programs may call different computer malwares the same name where providing just the name of a virus is not sufficient where this takes corrective action after a technique by which multiple names of a given virus can be determined in a quick and automated fashion (Gryaznov-col.1, lines 24-35 and 52-61). Therefore, examiner have combined proper and relevant prior arts for a person of ordinary skills in the computer technology art to read on the claimed invention.